NISSC Workshop

Common Criteria

Protection Profiles

Lynne Ambuel

Murray Donaldson

Who are we ...

... and why are **WE** here ?

- Lynne Ambuel
  - BDM International
  - CC Project Technical + Executive Support

- Murray Donaldson
  - CESG, UK
  - CC Project Coordinator

Purpose

- Understand Common Criteria
- Gain understanding of process for
- Assumed basic knowledge of Security

What this is Not

- Tutorial on Computer Security
- Discussion of Merits of CC
- In Depth Analysis of CC

Agenda

- Overview of Protection Profiles and

- How to Fill in Sections of PPs/STs
- Use Examples to Clarify

Terminology

- PP - Protection Profile
- ST - Security Target
- TOE - Target Of Evaluation
- TSF - TOE Security Functions

Stop us as we go ....

Overview

- What is a PP?
- What is a ST?
- How are they used?
- How are they Related?

Protection Profile Definition

- Complete Set of Functional and Assurance Requirements to Address an Identified set of Security Objectives

- Reusable Set - Abstract to be Met by Various Implementations

- Statements of Wants and Needs

Security Target Definition

- Developer Response to Statement of
- Contains Requirements Similar to PP
- Specific Set - Based on Implementation
- Statement of “I Provide”

Protection Profile Usage

- Users (User Advocates) - State Real-World Requirements
- Developers - Gauge Market
- Research/Academia - State Good Security Sets
- Evaluators - Have Basis to Assess

Security Target
Usage

- Users (User Advocates) - Compare Implementation to Stated Needs

- Developers - Communicate Provision

- Evaluators - Basis for Assessing
  - Basis for Resource

PP/ST Relationship

- “I want” vs “I provide”
- Generic vs Specific
- Requirements vs Specifications

- ST can be in Response to no PP - Developer states they meet requirements that customer has yet to

Protection Profile Structure

- Descriptive Front Matter
- Intended (Generic) Environment
- Security Objectives
- Requirements to Meet Objectives
- Rationale of How Requirements Meet

Security Target Structure Additional Information

- Summary Specification
- PP Claims
- Rationale
  - How requirements meet objectives
  - How provisions meet requirements

How Do You Start

- Know General Security Objectives
- Build on Work of Others or Start from

Illustrative Examples

- Actual Examples will Enhance Understanding
- Will Use these as Go through Building

Example - Description - 1

Application Gateway Firewall (AGFW) PP

- Firewall providing control over access to network resources at application level
- Limited to Internet firewalls
- Intended environment assumed to comprise
  - private network
  - hostile network

Example - Description - 2

Role-Based Access Control (RBAC) PP

… permit multiple users to perform a variety of functions based on defined roles, which allow controlled, shared access to data and IT

Example - Description - 3

Controlled Access PP (CAPP)

… based on the C2 class of the TCSEC (DOD 5200.28-STD).

PP/ST Structure

- Determining Descriptive Material
- Describing the Security Environment
- Determining the Security Objectives

PP/ST Structure Introduction

- Identify PP
- Abstract Short Description

Example - Identification

- Title: Role-Based Access Protection.
- Registration: <to be completed on registration>.
- Keywords: Access control, role-based access, separation of duties, least privilege, information protection

Example - Abstract

- In general terms, a firewall can be used to control the access that one network has to another, by forcing all interactions to pass through the firewall. The firewall can then decide whether particular interactions are to be permitted based on the apparent source of the request and the nature of the request.

PP/ST Structure
TOE Description

- Product Type
- Intended Usage
- General IT Security Characteristics

Example TOE Description

- The TOE is an Internet firewall providing application/proxy gateways.
- A network comprising a large number of hosts is difficult to manage......
- A firewall may be used to limit the access .... the hostile network has to the private

Example TOE Description (contd.)

- It is assumed ..... to limit the exposure of the
- It is also assumed .... hostile network limited access .... constrained ....network vulnerable

PP/ST Structure
Security Environment

- Threats Intending to Address/Counter
  - Threat Agent
  - Attack
  - Asset
- Description of Organisational Security Policies
- Secure Use Assumptions

Example - Threats 1 of 3

- Threats labelled T1 to T5
  - T1-T4 posed by attacker on hostile network
  - T5 covers impersonation of firewall
- Example threat defined in AGFW PP
  - *An attacker on the hostile network may exploit flaws in service implementations to gain access to hosts or other services*

Example - Threats 2 of 3

- Where
  - threat agent = *attacker on the hostile network*
  - IT assets = *hosts or other services* on the private network
  - form of attack = *exploit flaws in service implementations*

Example - Threats 3 of 3

Threats not countered by TOE (TE1 - TE6)

- Attack from hostile users on private
- New, previously unknown, attack
- Viruses
- Negligent/hostile administrators
- Physical attack on firewall

Example - Threats 1 of 3

- Threat T.ACCESS
  - *A user may gain access to resources or perform operations for which no access rights have been granted.*

Example - Threats 2 of 3

- Where
  - threat agent = *user on the system*
  - IT assets = *operations or data* on the
  - form of attack = *exploit services and facilities which are unprotected*

Example - Threats 3 of 3

Threats not countered by TOE

- T.ROLEDEV
  - *The development and assignment of user roles may be done in a manner that undermines*

Example - Organisational Security Policies - 1

Application to AGFW PP

No organisational security policies defined

- Firewall configurable
- Imprecise policy would not add value to

Example - Organisational Security Policies - 2

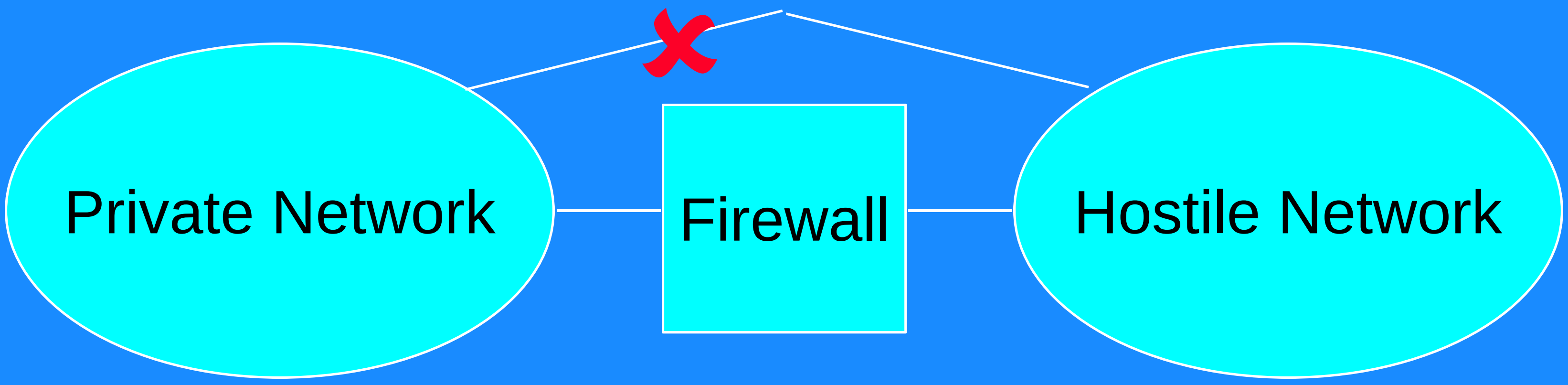
Application to Controlled Access PP

- *.. the organizational security policy described below is drawn from Manual 5200.28-M … it applies to many non-*

- P.KNOWN
  - *Legitimate users of the TOE must be identified before TOE access can be granted.*

Example - Secure Usage Assumptions

- Example 1 from AGFW PP
  - *The firewall must be configured as the only network connection between the private network and the hostile network.*



Example - Secure Usage Assumptions

- Example 2 - Controlled Access PP
  - *Competent individuals to manage the TOE and the security of the information it*
  - required to maintain the operational integrity of the system

Example - IT Security Objectives - 1

- RBAC - O.DUTY
  - *The TOE must provide the capability of enforcing ‘separation of duties’.*
  - Enforces through roles that restrict users to a subset of operations on specific data

Example - IT Security Objectives - 2

- Controlled Access - O.OPERATIONAL_ASSURE
  - *Allow a site to periodically validate the correct operation … (hardware and*
  - That the underlying platform is still providing the correct services.

Example - Non-IT Security Objectives

- O.INSTALL
  - *Those responsible for the TOE must ensure that the TOE is delivered, installed, managed and operated in a manner which maintains IT*

IT Security Requirements

- Functional
- Assurance

Choosing Functional Requirements

- Functional Requirements:

  Desired Security Behaviour of IT that can be observed by Investigating a TOE

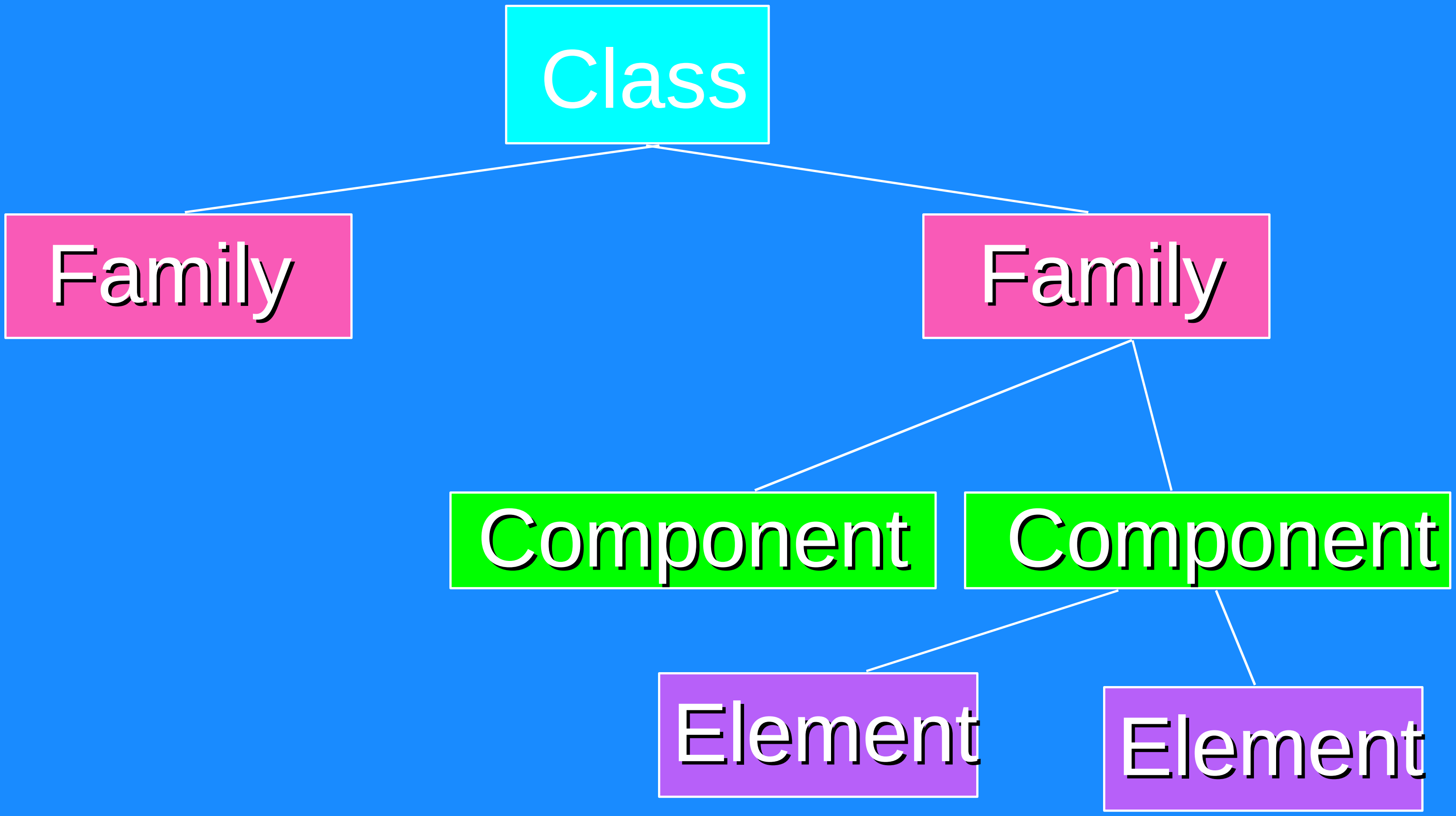
Requirements & Operations

- Choosing Functional Requirements
- Operations on Functional Requirements
- Completeness, Consistency & Technical Soundness

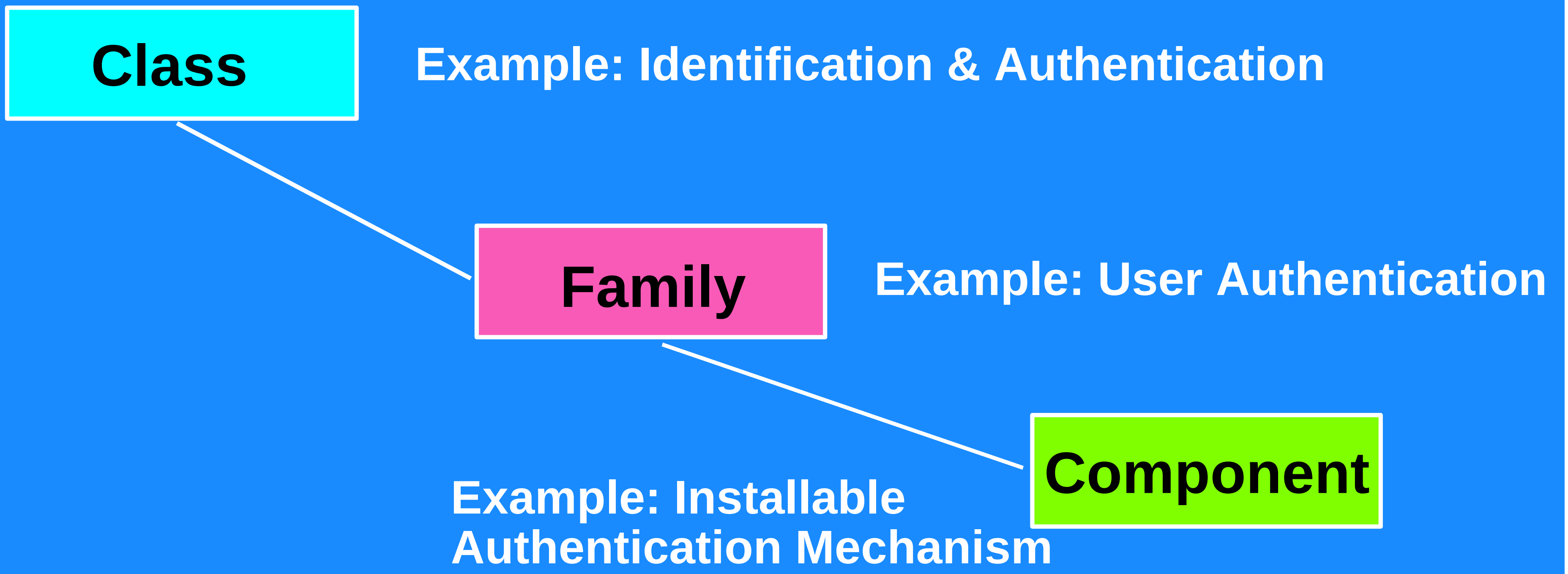
Common Set of Functional Requirements

- Part 2 of the Common Criteria
- Agreed to as Useful and Evaluatable

Requirements Structure



Requirements Example



Class

Example: Identification & Authentication

Family

Example: User Authentication

Component

Example: Installable Authentication Mechanism

Functional Requirements Classes

- High Level Organising Principle
- Contains Families of Common Intent or Approach to Meet Objectives
- Families in Class Differ in Coverage of

Functional Classes

- Security Audit (FAU)
- Communication (FCO)
- Cryptographic Services (FCS)
- User Data Protection (FDP)
- Identification and Authentication (
- Security Management (FMT)

Functional Classes (cont.)

- Privacy (FPR)
- Protection of the Trusted Security
- Resource Utilisation (FRU)
- TOE Access (FTA)
- Trusted Path (FTP)

Functional Requirements Families

- Contains Sets of Security Components
- Components in Family Share Security

- Components in Family Differ in Rigour or Emphasis

Class FIA - Identification and Authentication

- FIA_ADA - User Authentication Data Administration
- FIA_ADP - User Authentication Data Protection
- FIA_ATA - User Attribute Administration
- FIA_ATD - User Attribute Definition

Class FIA - Identification and Authentication (cont.)

- FIA_SOS - Specification of Secrets
- FIA_UAU - User Authentication
- FIA_UID - User Identification
- FIA_USB - User Subject Binding

Functional Requirements Components

- Contains List of Evaluatable Statements "Elements"
- Organised in Relationships within Family
- Either Hierarchical or Non-Hierarchical

Functional Requirements Components - Hierarchy

- Offers “More Functionality”
  - Additional Functions
  - Offers Function to More Users

Satisfying Dependencies

- Some Requirements Cannot be Met Without Existence of Other

- Example: Cannot Audit Identification of User if Never Identified

Choosing Functional Components - Example

- Choose Components
- Resolve Dependencies

Choosing Functional Components - Example direct

- RBAC - O.DUTY (separation of roles)
  - FDP_ACF.1 (Security attribute based access
  - FIA_USB.1 (User subject binding)
- “C2” - O.OPERATIONAL_ASSURE (application proxy authentication)
  - FPT_AMT.1 (Abstract machine testing)

Choosing Functional Components - Example dependency

- Additional RBAC supportive requirements e.g.
  - FPT_RVM.1 (Non-bypassability of TSP)
  - FPT_SEP.1 (TSF domain separation)

Choosing Functional Components - Example dependency

- RBAC Dependencies FDP_ACF.1 -
  - FDP_ACC.1 (Subset access control)
  - FMT_MSA.3 (Static attribute initialisation)
- Audit
  - *basic* level selected

Customising Functional Requirements

- Flexibility to Tailor Functional Requirement Components from Part 2
- Through operations
- Three Types of Operations
  - Assignment
  - Selection
  - Refinement

Assignment Operation

- Specification of a parameter filled in when component is used
- “Fill in the Blank” operation
- Allows PP/ST writer to provide information relating to application of the

Assignment Operation e.g. FAU_SEL.1.1

- The TSF shall provide the capability to include or exclude set of audited events based on the following
- [Assignment: *List of additional attributes*] that audit selectivity is based upon.

Selection Operation

- Specification of elements selected from a list given in the component
- "Multiple Choice" operation
- Allows PP/ST writer to select from a provided list of choices

Selection Operation e.g. FAU_SEL.1.1

- The TSF shall provide the capability to include or exclude
  set of audited events based on the following

- [Selection: *object identity, user identity, subject identity, host identity, event type*]

Refinement Operation

- Addition of detail to component
- “Essay Question” operation
- Allows PP/ST writer to specify additional ***narrow*** the scope of a functional requirement

Refinement Operation e.g. FIA_UAU.1.1

- The TSF shall authenticate any user’s claimed identity.
- The TSF shall authenticate any user’s claimed identity *using biometric techniques.*
- The TSF shall authenticate any user’s claimed identity *using retinal scan techniques.*

Example

- Operations
  - Assignment - FIA_AFL.1.2
  - Selection - FAU_GEN.1.2
  - Refinement - no refinements at this time

Example - Operations

- Assignment - FIA_AFL.1.2
  - When the defined number of unsuccessful authentication attempts has been met or *terminate the user session establishment process*.

Example - Operations

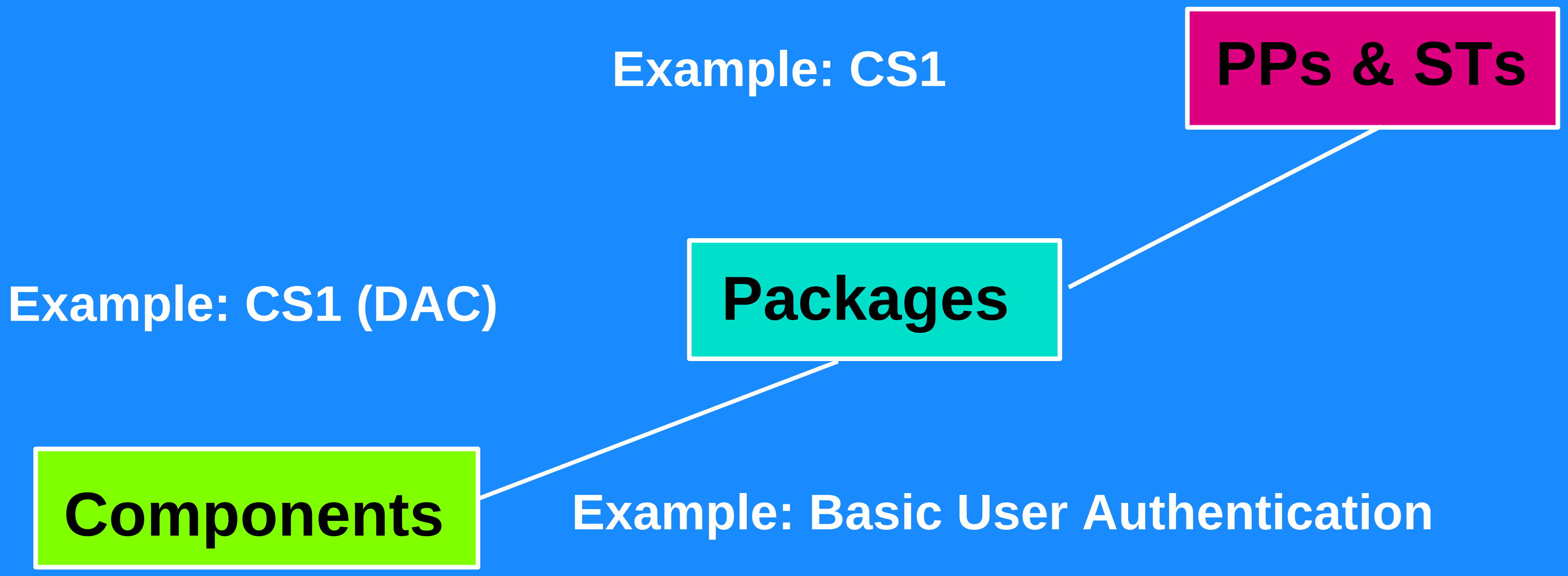
- Selection - FAU_GEN.1.2

  The TSF shall record within each audit record at least the following information:

  - Date and time of the event, type of event, subject identity, and *success or failure* of the event; and ......

- Refinement - no refinements at this time

Requirements Composition



Example: CS1

PPs & STs

Example: CS1 (DAC)

Packages

Components

Example: Basic User Authentication

Example Composability

Firewall based on underlying O/S

- Minimum requirement on firewall
  - direct implementation of security objectives
- Additional requirements on IT environment
  - supporting requirements only

Example Composability

- Firewall implements
  - FTA_TSE.1 (TOE session establishment)
  - FAU_GEN.1 & FAU_ARP.1 (audit/alarms)
  - management of parameters/attributes
- OS *may* implement
  - storage/protection of audit trail
  - firewall administrator authentication

Rationale for Requirements Chosen

Need to Consider Whether:

- Objectives address environment
- Requirements address Objectives
- Consistency
- Completeness
- Technical Soundness

Example

- Rationale
  - Sample Objectives
  - Sample Suitability
  - Sample Dependency
  - Sample Completeness

Example - Rationale
Sample Objectives

Approach taken

- Map security objectives onto threats
  - in tabular form (AGFW PP)

- Justify suitability of objectives for each
  - *T2 An attacker on the hostile network may exploit inappropriate use of service protocols*
  - *O2 and O3 limit the hosts and service ports that can be accessed from, respectively, the hostile and private networks. O6 monitors possible attacks, providing the firewall administrator with the means of detecting them and hence taking appropriate action.*

Example - Rationale
Sample Suitability

Approach taken

- Map functional requirements onto security objectives
  - in tabular form RBAC, Controlled Access and AGFW PP

Example - Rationale
Sample Suitability (contd.)

- Justify suitability of each objective, e.g.
  - *O1 The firewall must limit the valid range of addresses expected on each of the private and hostile networks*
  - *FTA_TSE.1 provides the capability of limiting access in the manner required by .1 ensures that this function is always invoked when required.*

Example - Rationale Sample Dependency

Approach taken

- Assign each functional component a
- Draw up a table covering all functional

PP Component		Dependent on	
Number	**Name**	**Name**	**Reference**
1	FAU_GEN.1	FPT_STM.1	27
10	FIA_ATD.1	None	-

Example - Rationale
Sample Completeness

- Build on dependency analysis
- Show defence against bypassing & tampering
  - tabular form
  - supported by explanation of general

  - *Tampering attacks are prevented by .....*

Example - Rationale
Sample Completeness (contd.)

- *FPT_SEP.3 which maintains domain separation, preventing external tampering with the security functions*
- *Security functions which restrict the modification of attributes to administrator e.g.*

IT Security Requirements

- Functional
- Assurance

Choosing Assurance Requirements

- Assurance Requirements:

  Assurance is an attribute of an IT product or system which permits those depending on the IT product or system to have confidence that the security features enforce the security policy.

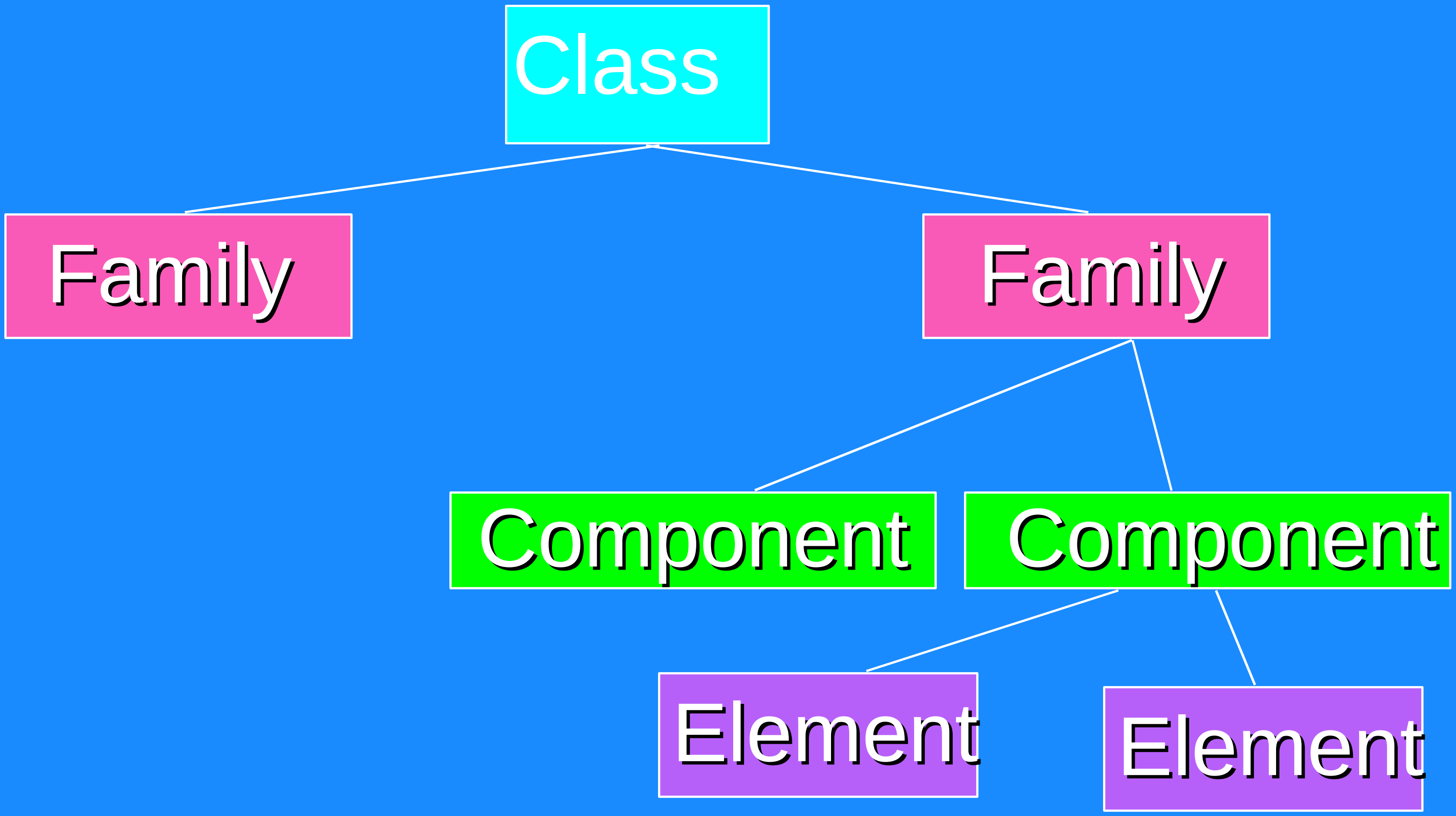
Requirements & Operations

- Choosing Assurance Requirements
- Operations on Assurance Requirements
- Completeness, Consistency & Technical Soundness

Common Set of Assurance Requirements

- Part 3 of the Common Criteria
- Agreed to scale for measuring assurance

Requirements Structure



Class

Family

Family

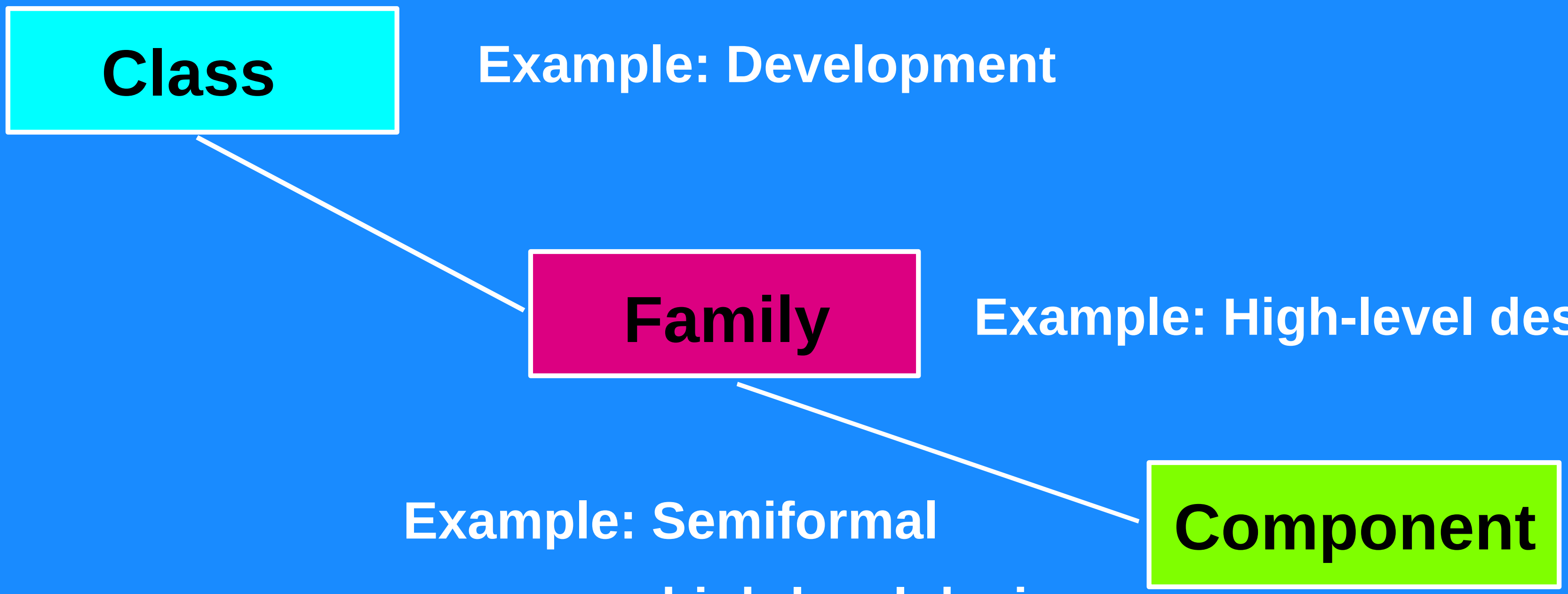
Component

Component

Element

Element

Requirements Example



Class

Example: Development

Family

Example: High-level design

Component

Example: Semiformal

high-level design

Assurance Requirements Classes

- High Level Organising Principle
- Contains Families of Common Intent or Approach to Meet Objectives
- Families in Class Differ in Coverage of

Assurance Classes

- Configuration management (ACM)
- Delivery and operation (ADO)
- Development (ADV)
- Guidance documents (AGD)
- Life cycle support (ALC)
- Tests (ATE)
- Assurance Maintenance (AMA)
- Vulnerability assessment (AVA)

Class ADV - Development

- ADV_FSP - Functional specification
- ADV_HLD - High-level design
- ADV_IMP - Implementation representation
- ADV_INT - TSF internals
- ADV_LLD - Low-level design
- ADV_RCR - Representation correspondence

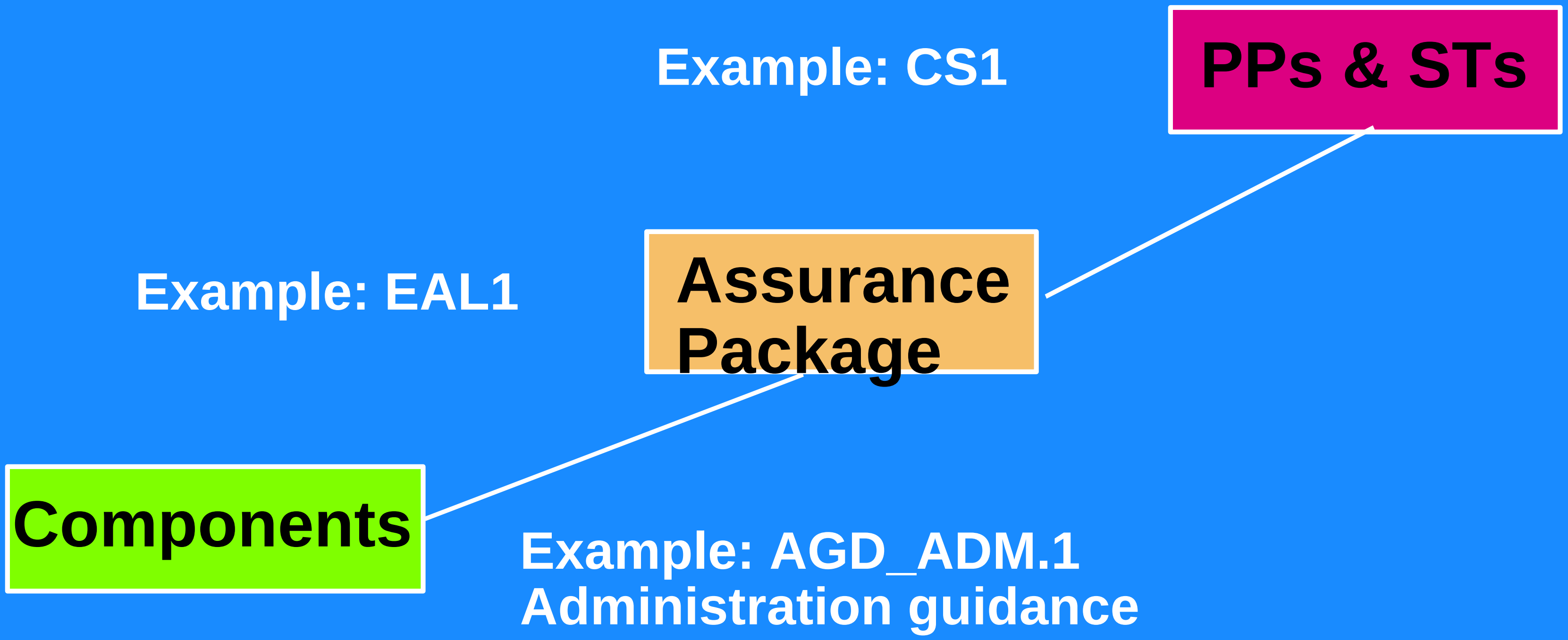
Assurance Requirements Components

- Contains List of Evaluatable Statements “Elements”
- Organised in Relationships within Family
- Hierarchical

Assurance Requirements Components - Hierarchy

- Offers “More Assurance”
- Additional Requirements
- Offers More Rigour
- Security-based

Requirements Composition



Example: CS1

PPs & STs

Example: EAL1

Assurance Package

Components

Example: AGD_ADM.1
Administration guidance

Predefined Evaluation Assurance Packages

- Evaluation Assurance Levels (EALs)
- Uniformly increasing scale, seven levels
- Assurance obtained is balance of cost

- Achieved by substitution and addition
- Possible to represent other combinations

Evaluation Assurance Levels EAL1

- Evaluation is meaningful and economically justified
- Detect obvious errors with minimum
- Not likely to find deliberate subversion
- Applicable where risk is not serious

Evaluation Assurance Levels EAL2

- Minimal additional developer tasks
- Low-Moderate assurance
- Useful for evaluating legacy systems

Evaluation Assurance Levels EAL3

- Moderate level of assurance
- Thorough investigation of product and

- Maximum assurance with positive security engineering
- Without substantial alteration of sound development environment

Evaluation Assurance Levels
EAL4

- Moderate-High level of assurance
- Rigorous development practice
- No “specialist knowledge, skills or other resources” required
- Highest level likely for retrofit of an
- Some additional engineering cost

Evaluation Assurance Levels EAL5

- High assurance, risk situations
- Rigorous commercial development
- Moderate use of specialist engineering
- No unreasonable development costs

Evaluation Assurance Levels EAL6

- High assurance, specialist security

- High value assets, risk situations
- Rigorous development environment
- Application of security engineering

- Justified additional development costs

Evaluation Assurance Levels EAL7

- Maximum assurance for practically
- Extremely high risk situations
- Justified higher development environment costs
- Focused security functionality
- Formal analysis

Requirements Composition “Rules”

- Dependencies
- Hierarchical Relationships
- Operations

Dependencies

- Same as Part 2
- Identify other components on which this component is dependent

Hierarchical Relationships

- Not Like Part 2
- Assurance Component Hierarchies Are
- Component N+1 is Hierarchical to

Customising Assurance Requirements

- Through operations
- Flexibility to tailor components and assurance packages
- Two Types of Operations
  - Refinement (on components)
  - Augmentation (on assurance packages)

Refinement Operation

- Refinement
- e.g.
  - The CM system shall provide an automated means to ensure that only changes are made to the TOE implementation representation. *This shall be compatible with SCCS.*

Augmentation Operation

- Flexibility to tailor Assurance Packages
  - Evaluation Assurance Levels from Part 3
- Meet specific needs
- Specify Part 3 assurance component(s) in addition to those in an Assurance

  - higher component in the same family
  - component from another family

Example

Decision based on

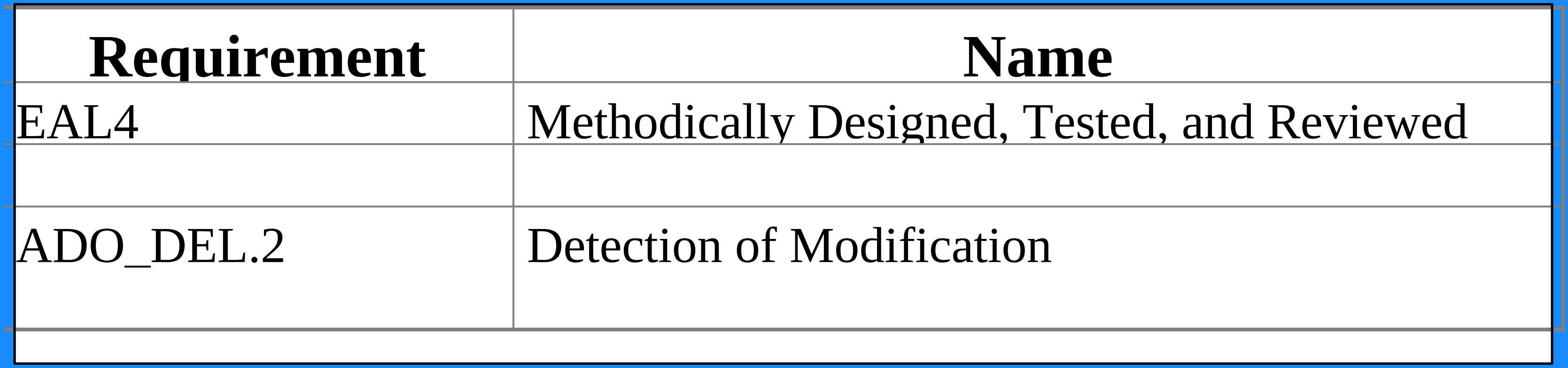
- Nature/level of threat
- Value of IT assets
- Technical feasibility

For the AGFW PP

- EAL4 selected
- No augmented assurance requirements

e.g. Augmentation

- Delivered in a known secure state
- Detection of any modification



Requirement	Name
EAL4	Methodically Designed, Tested, and Reviewed
ADO_DEL.2	Detection of Modification

IT Security Requirements

- Functional
- Assurance
- ……… and there’s more !

Extended Requirements

- Allowed in a ST and PP
- Functions and Assurance
- Flexibility to prescribe requirements
  - not contained in either Part 2 or Part 3

Rationale for Requirements Chosen

Need to Consider Whether:

- Objectives address environment
- Requirements address Objectives
- Consistency
- Completeness
- Technical Soundness

Example - Rationale Sample

- Assert EAL4 is known set of components:
  - mutually supportive and internally consistent
  - for which dependencies are satisfied
- Assurance always supports functionality
- Justify assurance level chosen
  - EAL4 requires no specialist techniques
  - defence against sophisticated attacks: must have access to low-level design / source code

e.g. - Rationale Sample

- ADO_DEL.2 - Detection of Modification
  - Added threat that the TOE may be modified before delivery
  - The security objective is to protect the integrity of the TOE
  - The non-IT environment provides procedures and measures to detect modification, as defined in the environmental policy

Security Target Additions

- Claim of compliance with a PP
- ST Summary Specification

PP Compliance Claim

- List of PPs that an ST Claims to Meet
  - None
  - Simple Reference to PP(s)
  - Qualified Reference to PP(s)
  - Extension to PP(s)

Example - Compliance Claim

- Show all PP requirements covered
  - ST requirements included where different
  - Mapping of functions onto requirements shown in tabular form
- Show all PP operations completed
  - demonstrated by means of table

Example - Compliance Claim

- Justify PP additions
  - 3 additional functional requirements
  - justified why supportive of other

  - additional dependencies shown to be

Summary Specification

- Security Functions to meet requirements & how
- Security Mechanisms/Techniques to meet requirements & how
- Security Assurance Measures to meet requirements & how

Example - Summary Specification

- Example 1 (AC_1)

  The TOE will control access on the basis of

  - *apparent source IP address or host name*
  - *apparent source port number*
  - *destination IP address or host name*
  - *destination port number*

Example - Summary Specification

- Example 2 (AC_3)

  The following proxies are supported, which support access based on source and

  - *telnet*
  - *http*
  - *etc.*

Example - Summary Specification

- Example 3 (TSF_6)

  The firewall administrator, and only the firewall administrator, can perform the following

  - *display and modify the firewall access control*
  - *initialise and modify user authentication data*
  - *etc.*

PP & ST - What Next ?

- 2 Aspects of Assessment
  - Technical - evaluation
  - Business case - vetting
- Technical evaluation - Part 3
- Certification
- Mutual Recognition / Social Process

PP Evaluation

Evaluation Criteria for PPs

Protection Profile evaluation (Class APE)

- APE_DES - TOE Description
- APE_ENV - Security Environment
- APE_INT - PP Introduction
- APE_OBJ - Security Objectives
- APE_REQ - TOE Security Requirements

ST Evaluation

Evaluation Criteria for STs

Security Target evaluation (Class ASE)

- ASE_DES - TOE Description
- ASE_ENV - Security Environment
- APE_INT - PP Introduction
- ASE_OBJ - Security Objectives
- ASE_PPC - PP Claims
- ASE_REQ - TOE Security Requirements
- ASE_TSS - TOE Summary Specification

Workshop Summary

Summary

- CC Provides Vehicle for Stating IT Security Requirements
- PPs Contain Requirements and Justification for Requirements
- STs Contain Implementation Response to IT Security Needs
- CC is a Tool but Not a Panacea

What’s Next? - links

Contact - Secure WEB site

- Common Criteria Support Environment
  - ccse.cesg.gov.uk/

What’s Next? - links

- Where to get more information
  - Interim Protection Profile Registry
  - Protection Profiles in development
- Contact - WEB site
  - www.radium.ncsc.mil/tpep/library/protection_profiles
  - csrc.nist.gov/cc/pp/pplist.htm
  - www.cesg.gov.uk/cchtml/ippr/

What’s Next? - links

- CC reminder ………………...

- Contact - WEB site
  - http://www.cse.dnd.ca/cse/english/cc.html
  - ftp://ftp.cse.dnd.ca/pub/criteria/CC1.0
  - http://www.tno.nl/instit/fel/refs/cc.html
  - http://www.cesg.gov.uk/cchtml
  - ftp://ftp.itsec.gov.uk/pub/ccv1.0
  - http://csrc.nist.gov/cc

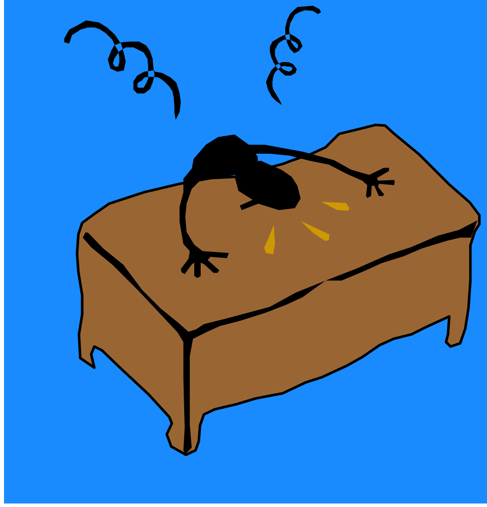
What is Next - contacts !

Send E-Mail! Contact addresses ……...

- criteria@cse-cst.gc.ca
- ssi20@calva.net
- cc@bsi.de
- criteria@nlncsa.minbuza.nl
- criteria@cesg.gov.uk
- criteria@nist.gov
- common_criteria@radium.ncsc.mil

Thankyou for your kind attention

Have a safe journey home ……



Whew ……..